MOVING TARGET DEFENSE

New Perspectives January 14, 2012

Proactive Cyber Defense

A New Moving Target Defense Strategy

A Coronado Group Perspective

Moving target defense (MTD) technology changes the cyber security game by wresting the advantage from the attacker by turning static systems into dynamic, moving targets. In MTD-enabled environments, attackers have to work harder to get in, are robbed of time to exploit vulnerabilities, figure out how the systems work making launching attacks riskier with lower odds of success.

SCIT-Based Moving Target Defense

Coronado Group is using patented SCIT technology to build state of the art, pro-active and cost-effective MTD cyber defense solutions that can be implemented now without making changes to your systems or compromising your current cyber security investment.

SCIT-MTD takes advantage of multi-core, virtualized environments turning them into dynamic moving targets. Using a combination of ultra-low persistence times and configurable virtual machine (VM) rotation times, the attack surface of your systems is continuously changed. To the attacker, the system appears static; under the covers, the VMs are being continuously rotated, returning to a pristine state a configurable intervals as low as a minute.

SCIT-MTD can be implemented quickly without making changes to your existing information systems or security infrastructure. SCIT-MTD removes malware without having to know its signature or detect is presence. It can be implemented now, it's cost effective, and it will dramatically improve your security.

A New Weapon in the Cyber Security and Digital Asset Protection

Traditional MTD Approaches Don't Work

MTD strategies call for making the attack surface of software appear chaotic and unpredictable to adversaries, forcing them to increase the work effort to exploit vulnerabilities for every desired target and lowering the odds of success. The theory is that by the time an adversary discovers a vulnerability in a service, the service will have changed its attack surface area so that another exploit against that vulnerability will be ineffective.

Emerging MTD strategy presents two significant challenges to adoption. First, MTD can't compromise performance and user productivity. MTD is built on complex processes involving memory address randomization, network address shuffling, data complexity, routing remapping and more. All have the potential to require more resources just to deliver the same performance. Most customer facing systems don't have the luxury of adding security that slows down performance for fear that potential users will simply move on if they experience slower response times. MTD approaches that work must be able to maintain performance and provide higher levels of protection.

The second challenge is the need to adding complexity just to enhance security. Adding more complexity to today's already complex system environments is anathema for most information technology professionals. Injecting chaos to the complex, distributed systems simply to foil intruders isn't a viable option for many organizations because of cost, impact on service delivery life cycles, and the prospect of adding new unknown vulnerabilities in the process. Enterprise software applications and the emergence of big data sets render the "add complexity" MTD security approach infeasible.

Cloud service and SAAS product providers may not have the luxury of adding complexity to applications and data they don't directly control. On demand provisioning of resources and highly distributed architectures to a wide range of diverse clients with different needs require strategies that don't require direct interaction and modification with digital resources to deliver solid security.

Coronado Group offers a different approach for delivery of proactive MTD solutions.

Read further to learn how SCIT-MTD works, what it takes to implement SCIT-MTD, and how to get started.

Self-Cleaning Intrusion Tolerance
How SCIT Works

SCIT-MTD
Self-Cleaning Intrusion Tolerance-Moving Target Defense

A new way to level the playing field between you and cyber attackers who want your data and your systems.

Self Cleaning Intrusion Tolerance (SCIT) is a patented technique for providing ultra-low intruder persistence time and continuous rotation of VMs to a pristine state to remove malware and rob intruders of the time needed to plan and launch attacks. Coronado Group uses SCIT to create robust, fast, and easy to implement moving target defense solutions that don't require changes to existing information systems, applications, or security protocols to deliver a new high level of protection.

SCIT technology is based on the premise that intrusions are inevitable. Rather than assuming you can prevent every intrusion and keep all the bad guys off your system, the SCIT-MTD approach assumes that someone is going to get in one of these days. When intruders get in, you need to throw them out as quickly as possible without waiting to figure out what they are up to. SCIT-MTD assumes that while intrusions are inevitable, the bigger problem is that intruders are in your systems for a very long time watching how your systems work. Once they are in they are learning how your systems operate, where your most valuable assets are located, and how to get your data out of your system under your security radar. Advantage intruder.

SCIT-MTD is designed to fight this asymmetric information advantage of your adversaries. They know about you - you don't know anything about them until it's too late.

SCIT-MTD takes advantage of multi-core virtualized environments using the system's architecture as a weapon in cyber defense. SCIT-MTD provides a straight forward approach to security. SCIT-MTD helps change the cyber war battlefield.

How SCIT-MTD Works

SCIT Moving Target Defense continuously changes the attack surface making it difficult to get in and if they get in do not have the time to launch an attack. Using virtualization technology, SCIT-MTD rotates pristine virtual servers and applications at configurable intervals as low as every minute, or less.

In a typical implementation, at any given time, there are five servers online and three servers being wiped clean. Eventually every server will be taken offline, cleaned and restored to its pristine state.

"Hackers have repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Market... The exchange's trading platform—the part of the system that executes trades—wasn't compromised. However, it couldn't be determined which other parts of Nasdaq's computer network were accessed."

Wall Street Journal, February 11, 2011

The speed of rotation means that the adversary won't be able to persist in the system and exploit the vulnerability fast enough to persist in the environment. Forcing the adversary to make repeated will raise visibility to traditional detection and monitoring capabilities.

If an attacker is able to place malware on a server, the malware will be deleted without reliance on the signature based detection process. SCIT-MTD allows systems to continue working through an attack, with automatic and rapid recovery to a clean state.

The Benefits of SCIT-MTD

- Servers are restored to a pristine state based on configurable rotation times as low as every minute;
- SCIT-MTD parameters tailored based on the security posture of your digital assets - high value assets can have different parameters than low value assets;
- Malware is deleted without the need to detect it or know it's signature;
- Attacker visibility is increased by forcing the attacker to apply multiple attacks in an attempt to gain access to digital assets;
- Increased security of user dense and application dense cloud environments;
- Near-real time management of digital assets supporting reconfiguration and application of patches and upgrades without rebooting servers supporting mitigation of zero day vulnerabilities;
- Elimination or reduction in server failures due to errors like memory leaks;
- Better planning of software deployment and patch management;
- Applications are harder to corrupt, disable or remove.

Hackers who appear to be based in China have conducted a "coordinated, covert and targeted" campaign of cyber espionage against major Western energy firms

The Wall Street Journal
February 11, 2011

The National Counter-intelligence Executive blamed China and Russia for stealing sensitive economic and commercial data threatening an estimated $400 Billion in spending on R&D

The Wall Street Journal
November 3, 2011

Make Intruders Work Harder

And Wage Cyber War Without Recon

Cyber warfare, like conventional warfare, relies on reconnaissance and intelligence. You can't fight a cyber war without knowledge of your enemy and their methods and tactics. Foiling cyber attacks requires strategies to rob your adversary of recon and make them work harder.

By the time most intrusions are discovered, attackers have been present in the system for long periods of time going undetected by conventions cyber security infrastructure. Intruders don't leave a trail so security professionals often have no idea where they have been or what the have stolen until the damage is done.

To exploit a system, an adversary must learn a vulnerability and hope that it is present long enough to exploit. Most attacks exploit more than one vulnerability. Attackers need the ability to observe the operation of key IT systems over long periods of time. They need the opportunity to map out an inventory of assets, vulnerabilities, and potential exploits before they can launch an attack. Attackers can afford to invest significant resources in developing attacks since the attacks can often be used repeatedly from one system to another.

After decades of information system practices focused on standardization, and replication of servers, standardized applications, desktops, browsers, technology built around three operating systems and extensive reuse of code and access practice we have turned our systems into sitting ducks. Then add the 24/7/365 exposure of mission critical corporate information systems to the internet and you have the optimal environment for intrusions and compromise of important assets. Moving target defense offers new tools that make your enemy wage cyber war without the benefits of recon. Static systems give attackers a substantial advantage.

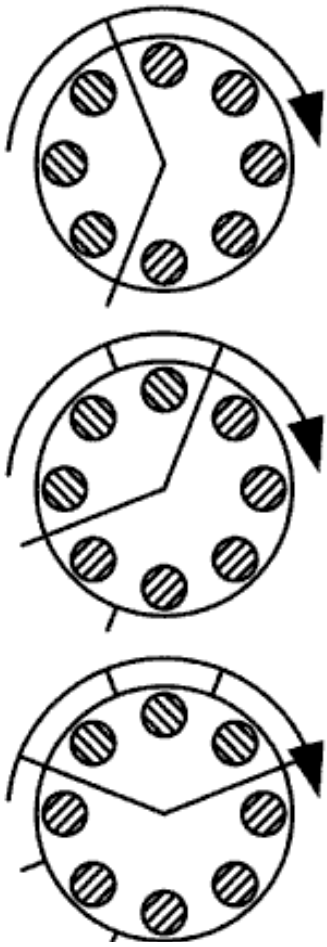
SCIT-MTD increases the work effort of the attacker by limiting the time available for launching an attack or exploring system capabilities. The present of SCIT-MTD deterrence isn't visible to intruders forcing them to try again and again to gain access to your systems. This increases the visibility of an attack to conventional cyber security systems.

A typical attack requires several steps: reconnaissance to gain access, learn about the system and plan an attack, introducing malware into the environment and getting it to the place where it needs to be to work, and then executing an attack. Intruders who seek to steal data also need to exfiltrate the stolen assets.

SCIT-MTD makes each of these steps more difficult, thus increasing the attacker's work load and, in turn, visibility to cyber defense systems. This approach provides enhanced adversary denial and deception.

In a SCIT-MTD enabled environment malware would need to be changed, loaded, and executed in less than a minute to gain significant access to digital assets. Attackers are robbed of the ability to load malware, to upgrade malware, to execute programs, and steal data. As processors get faster, faster swapping will make malware deployment increasingly difficult in this environment.

SCIT-MTD supports a variety of deployment strategies that enable highly customizable rotation and protection schemes as well as the capability to create a continuously changing dynamic environment that recovers with resilience.



"...the speed and agility of adversaries as well as simple polymorphic mechanisms that continuously change the signatures of attacks renders signature-based approaches largely ineffective."

National Cyber Leap Year Summit 2009 Co-Chairs Report
September 6, 2009

One Minute Zero Day Vulnerability

No Signatures Required

What do you do when you don't know what you don't know?

One of the most vexing problems in cyber defense is the impact of zero day vulnerabilities. A Zero Day Vulnerability occurs when an unknown security hole is exploited. Once these risks are discovered the goal of cyber security professionals is to understand the security hole, build a patch that fixes the problem, deploy the patch to customers and users, and make sure system ALL the systems where the vulnerability exists are fixed.

Security experts try to maintain a quiet period where the holes are only known by a few people in an attempt to keep the security holes from being publicly disclosed. In today's hyper-connected real time world zero day vulnerabilities don't stay quiet for very long. And that's when the trouble begins.

SCIT-MTD enabled systems offer new protection from zero day vulnerability intrusions. SCIT-MTD's ultra-low persistence time removes malware and cuts down the time intruders can exploit the risk.

Even if there is a vulnerability attackers will need to try again and again to get into your system. As intrusion attempts go up so does the visibility of the attack in your cyber defense systems.

The ability to rapidly deploy new software is a built in component of SCIT-MTD. New software is added to the pristine servers that rotate to deliver MTD capabilities and it is automatically deployed without system disruption.

SCIT-MTD enabled systems are substantially more secure even if there are vulnerabilities present because the timeframe that the attacker has to exploit the vulnerability is equal to the time it takes to trigger a new server rotation. Organizations can implement faster and more complex rotation schedules while a vulnerability exists adding another layer of security until the vulnerability is patched.

Q&A

On Implementing SCIT-MTD

What does it take to implement SCIT-MTD?

Coronado Group works with you to develop a SCIT-MTD Asset Protection Profile. This defines the assets you want to protect; how frequently you need to rotate your VMs to achieve the level of protection you want, what level of forensics you want and how you want the system to handle your compromised servers - some systems operate totally unattended rotating continuously, others rotate to a clean VM based on alerts from your SIEM. Once we have the profile, we install and configure SCIT-MTD. Your system is protected.

My systems are already complex. Adding new complexity at the application and system level isn't feasible. Can I still implement SCIT-MTD?

Yes. SCIT-MTD doesn't require any changes to IT infrastructure or applications other than the addition of a clean VM. SCIT-MTD uses the power of multi-core systems, virtualized environments and fast processors to rotate the VMs to a pristine state.

Does SCIT-MTD change the way my systems look to attackers?

No. In fact, an attacker won't have the advantage of knowing you are using SCIT-MTD because the system will appear static to wanna be intruders. The SCIT-MTD processes are transparent. Internal IP addresses change. External ones don't.

What about my existing investment in cyber security - IDS/IPS, firewalls, DMZs, and SIEM technology?

Nothing changes. You can still use those systems. SCIT-MTD makes these systems more valuable. First, because intruders have to try again and again to get in it raises the visibility of attacks. Second, it gets rid of hackers by booting them off the system as soon as they get on. There's no need to know the attacker's signature to remove them from your system. SCIT-MTD helps eliminate false positives making your current infrastructure more efficient. Finally, it improves over all performance of your security infrastructure by raising the visibility of serious threats and supporting higher rates of continuous monitoring without having to add more resources to do it.

Will SCIT-MTD add new tasks for my security team?

No. SCIT-MTD is fully automated when it's operating. Your team may find the new forensic information valuable and may want to use it to gain insight to what's going on with their systems and how to make security even tighter.

What happens during an attack?

SCIT-MTD enables your systems to work through attacks. SCIT continuously replaces the operating system, device drivers, and applications with a new pristine server. Compromised servers are replaced automatically. SCIT-MTD's automated clean up and recovery of server assets removes the residue from errors and cyber attacks automatically without human intervention.

Will my Cyber Security people be happy?

Yes. When SCIT-MTD is implemented with Forensics, you'll have near real-time snapshots of attacker profiles and methods. SCIT-MTD improves Incidence Response (IR) providing new tools to analyzing attacks. SCIT-MTD's near real-time forensic data offers a powerful tool for watching how attacks evolve. While the attacker is trying to figure out how to get back onto the system, your team will be implementing its defense strategy proactively and gathering intelligence about the intruder's methods and attempts. The regenerative aspect of SCIT-MTD supports in-attack software upgrade and maintenance with no downtime - keeping your systems up and your users happy. Machine generated reconstitution of compromised servers with high levels of corruption immunity and in-attack software repair and enhancement is another benefit. SCIT-MTD delivers powerful new tools. SCIT-MTD has two other benefits. It works great for patch management and automating software upgrades; and it helps control for memory leaks.

How Do I Get Started?
Use Our Quick Start Program

Coronado Group can work with you to explore how to deploy SCIT-MTD to protect your digital assets. We've designed our Quick Start program to get you up and running fast so you can see if SCIT-MTD works for you. We'll show you how it works on our fully functioning online store. You can trigger defacement and code destruction hacks recover automatically, you can launch your own attacks on our server.

We'll develop a comprehensive Asset Protection Profile to help you understand how to use SCIT-MTD for your systems. Coronado Group will show you how to implement MTD in your environment without having to change the information architecture of your your systems work. The Asset Protection Profile is yours even if you decide SCIT-MTD isn't for you. We have the tools to help you test and evaluate the system so you can focus on assessing the technology instead of figuring out how to test it.

After the assessment, we'll bring SCIT-MTD up on a five server configuration in your environment so you can take it for a test drive for 30 days and see how it works for your self. After the Quick Start we'll work with you to deploy SCIT-MTD to protect your digital assets.

SCIT-MTD Quick Start

Call us for a SCIT-MTD briefing and a conversation about your security goals.

Coronado Group will work with you on approaches to use SCIT-MTD to reach those goals.

Pick a test system you want to use to give SCIT-MTD a test drive.

Work with us to develop an Asset Protection Profile for that system so you can learn which SCIT-MTD options are best for you.

Implement the Asset Protection Profile configuration in a five server test environment.

See how it works for you.

Learn More About Proactive Cyber Security

Ask about our Cyber Security Aware Software Development Seminars

MOVING TARGET DEFENSE
Coronado Group, Ltd.
4938 Hampden Lane #436
Bethesda, Maryland 20814
www.coronadogroup.com

About Coronado Group

The Coronado Group, Ltd. is a specialized systems integration and professional services firm focused on helping its clients recognize and exploit the value of new and emerging technology to build solutions that work.

Coronado Group takes a proactive approach to cyber defense by designing and building in security before the programming starts. We provide cyber defense advisory services focused on cyber security, threat analysis and deterrence, agile and resilient cyber strategies, and emerging computer architectures. Coronado Group has implemented classified information systems and systems designed to manage privileged and highly sensitive trade secret and digital intellectual property.

Coronado Group can help you navigate the increasingly interconnected web of legal, regulatory, and statutory requirements to help you face the new reputational and economic risks directly related to how you create, distribute and manage your digital assets.

For more information

Contact Us

Please Call or Email
Arleen Zank

azank@coronadogroup.com

703.909.7722
301.986.1334 ext 109